# Segurança, privacidade e anonimato – guia avançado

Por **Gabriel Camargo** - 27/10/2022

*Créditos da imagem: Bit Notícias*

- Dicas e Pontos Gerais Para o Mundo Virtual
- Dicas e Pontos Gerais Para o Mundo Físico
- Softwares/serviços recomendados

O mais famoso ransomware, WannaCry, que ganhou grande notoriedade e trouxe ao público esse tipo de ameaça, para se disseminar ao redor do mundo, utilizou uma vulnerabilidade vazada por crackers do Shadow Brokers que obtiveram ferramentas da NSA. Esse exemplo indica o arsenal cibernético à disposição de ameaças complexas. Muito dinheiro é investido para a criação de ferramentas de penetração, vigilância e extração de dados. Muitos milhões de dólares são investidos para manter as agências de inteligência sempre um passo à frente. Com o avanço de contramedidas de privacidade e anonimato, no entanto, nem sempre elas conseguem. Novos métodos, então, começam a ser desenvolvidos, em um eterno cabo de guerra entre os que defendem e os que ameaçam a liberdade e autonomia do indivíduo.

O nível aqui apresentado é voltado para pessoas que ativamente lutam contra a elite coercitiva ou enfrentam adversários influentes e poderosos. Esse quinto artigo da série não é voltado para o público geral, sendo mais recomendado para uma fração específica de pessoas, como jornalistas em regimes autoritários. Mesmo com o aqui apresentado, adversários com orçamento virtualmente ilimitado e capacidade técnica altamente avançada podem obter sucesso em neutralizar seus inimigos. Os pontos

aqui expostos não serão suficientes para mitigar adversários com elevado nível de competência e fortes incentivos em silenciar vozes contrárias ao poder estabelecido. Contudo, mesmo não sendo suficientes, podem certamente auxiliar a correta mitigação de ameaças avançadas. Esse nível, então, mitiga completamente a capacidade de rastreamento de anunciantes e Big Techs, mesmo em smartphones. Também mitiga significativamente a capacidade de rastreio e vigilância realizada por agências governamentais.

Níveis mais baixos podem incorporar alguns dos pontos aqui apresentados. No entanto, quem está nesse nível deve tomar cuidado para não misturar ou confundir os diferentes compartimentos e meios de ação, quando adotadas medidas de níveis inferiores, principalmente no caso de serem mutuamente excludentes.

## Dicas e Pontos Gerais Para o Mundo Virtual

- Para conexões com JavaScript ativo, mesmo em VPN, é possível, caso utilizando um servidor localizado em país diferente ao da localização real, verificar diferenças na hora do dispositivo e da região da suposta conexão. Uma mitigação possível é a escolha de servidores presentes no mesmo país da localização real, ou a utilização de extensões como o NoScript para bloquear essas conexões;
- A utilização de VPNs e pontes dificulta, mas não impede que seu provedor descubra o uso da rede Tor. Seu uso, contudo, pode auxiliar nas conexões efetuadas em países hostis, dificultando o bloqueio;
- O uso concomitante da internet comum com conexões da rede onion, quando em VPN, pode dificultar, mas não impedir, a descoberta de quais sites estão sendo acessados, de acordo com os padrões de conexão;
- Por esse mesmo motivo, faça diferentes coisas simultaneamente enquanto conectado à rede Tor;
- Não use Tor e VPNs em redes fortemente monitoradas, como redes corporativas ou governamentais;
- Não use Tor e VPNs para acessar serviços presentes nas mesmas redes de onde se está acessando, como se conectar em uma rede corporativa para acessar serviços presentes nessa mesma rede. A capacidade de monitoramento do tráfego é substancialmente elevada;
- Você pode se conectar com a rede Tor por meio de uma VPN, ou por meio de mais VPNs em cadeia. Algumas VPNs também possibilitam o uso de mais de um servidor em simultâneo. Utilizar mais de uma VPN limita as informações que cada parte sabe sobre você. Se antes a única VPN sabia seu IP real e sua conexão à rede Tor, no caso de duas, nenhuma possuirá esse par de informações. A introdução de mais VPNs, contudo, aumenta a superfície de ataque e reduz a velocidade, além de necessitar confiança nos novos serviços utilizados;
- Mesmo quando comparado à cadeia de VPNs, a rede Tor proporciona maior grau de anonimato;
- Por ser uma rede com diferentes níveis de criptografia, que roteia o tráfego por diferentes nodos antes do destino, a rede Tor proporciona elevado nível de anonimato. Ataques que levem à descoberta da identidade real do usuário são possíveis, contudo, sendo por descuido ou por exploração de vulnerabilidade em sistema propício. Como a conexão é segregada entre diferentes nodos, cada um deles apenas consegue ver uma parta da conexão, nenhum sendo capaz de relacionar um determinado IP de origem a um IP de destino;

- Nodos maliciosos são descobertos com certa frequência na rede Tor, sendo posteriormente retirados do ar. Agências de inteligência estatal são conhecidas por rodas nodos maliciosos e tentar espionar o tráfego de usuários na rede. Mesmo com limitações e ataques possíveis, a rede Tor é uma das melhores alternativas atuais para a proteção da identidade de seus usuários, sendo utilizada mesmo pelas agências de inteligência estatais que tentam atacá-la;
- Para maiores níveis de proteção, sistemas operacionais recomendados são Tails, Qubes Os e Whonix. O sistema operacional Tails roda em um pendrive, sendo de fácil transporte e ocultação. Por ser um sistema amnésico, ao ser a mídia desconectada, todos os dados referentes à sessão são apagados, significativamente mitigando trabalho forense posterior. Por opção, pode-se guardar alguns dados de forma não amnésica, mas essa prática deve ser utilizada com cautela. Todas as conexões são efetuadas por meio da rede Tor. É recomendado reiniciar o Tails a cada troca de identidade, por exemplo, passando entre pseudônimos ou tarefas de diferentes escopos. Pode-se adicionar softwares ao Tails, mas deve-se tomar cuidado para que eles não comprometam a segurança configurada no sistema, por exemplo, ao instalar uma VPN;
- O sistema Whonix roda em máquinas virtuais, tendo sido projetado com avançadas contramedidas de segurança, privacidade e anonimato. Pode ser utilizado acima de um sistema Linux padrão, como Mint ou PopOs. Utiliza proteção por compartimentalização. Todas as conexões são efetuadas por meio da rede Tor. Consiste em duas máquinas virtuais, Gateway e Wokstation, sendo a interação do usuário realizada na segunda. Sempre inicie primeiramente a Gateway;
- Qubes OS é um sistema operacional que funciona como host do sistema, podendo, então, ser combinado com o sistema Whonix para maiores benefícios. Por utilizar extensamente a virtualização, com cada aplicativo rodando em uma máquina virtual diferente para garantir maior proteção, serão necessárias maiores capacidades de hardware para uma experiência agradável. Como exemplo, o mínimo de memória RAM recomendada é 16 GB. Das três soluções, o Qubes OS é o mais pesado. O Tails é o mais leve;
- Recomenda-se adicionar uma senha à BIOS/UEFI, bem como para os dispositivos de armazenamento do computador. Essas senhas podem ser configuradas na BIOS do sistema, sendo necessário inseri-las para realizar o processo de *boot* e acessar o sistema operacional instalado. Ainda na BIOS, caso houver essa opção, desabilite completamente o Bluetooth;
- Deve-se evitar o uso de serviços situados nos Estados Unidos, Canadá, Reino Unido, Austrália e Nova Zelândia, os membros dos Cinco Olhos. Também é recomendado limitar o uso de serviços presentes nos Nove e Quatorze Olhos: Dinamarca, França, Países Baixos, Noruega, Alemanha, Bélgica, Itália, Espanha e Suécia;

- Para dificultar a correlação de ações e posterior derivação de identidade, tente resolver Captchas, navegar em sites, mexer no mouse, rolar a página e digitar no teclado de modo sempre ligeiramente diferente, como com relação à velocidade e pausas;
- Mesmo a mais cara e complexa alternativa de privacidade pode ser mitigada pela mais barata e simples violência física cometida pelas forças estatais contra um indivíduo. Tenha planos de impossibilitar o seu acesso a dados críticos, caso peça a situação. Planeje o cenário de ser capturado e treine uma narrativa de negação plausível;
- Prevendo situações nas quais agentes coercitivos demandem suas credenciais, sob ameaça de cárcere, pode-se utilizar cofres criptografados ocultos. Cofres ocultos criados dentro de outros cofres não revelarão sua existência, mesmo quando o cofre principal for aberto sob ameaça. Para a criação desse tipo de armazenamento, utilize o software VeraCrypt. Caso bem-sucedido, os agentes coercitivos terão acesso apenas ao que você permitiu, mesmo eles pensando que obtiveram acesso a tudo;
- No VeraCrypt, para dificultar a descoberta de cofres criptografados, evite criar cofres grandes em arquivos que geralmente não possuem esse tamanho, como cofres de 20 GB em arquivos .jpg ou .png;
- Misture arquivos de cofres em pastas com arquivos de tamanho similar;
- Não nomeie seus cofres com nomes indicativos, como “cofre”, “secreto” ou “arquivos ocultos”;
- Evite criar cofres com tamanhos incomuns, como números redondos (20 GB, 50 GB). Tamanhos desse tipo são incomuns;
- Sempre desabilite a conexão automática das redes sem fio. Adversários podem criar redes com nomes idênticos, o seu dispositivo se conectando automaticamente caso as anteriores tenham sido salvas;
- Contra ataques sofisticados, a randomização do endereço MAC é insuficiente;
- É preferível salvar os endereços dos sites comumente visitados (fora do navegador, de maneira segura), para dificultar a entrada em sites falsos;
- Caso tenha dúvidas da legitimidade, digite suas credenciais de forma incorreta. Se o site aceitar, você saberá que é falso;
- Em suas contas, revise sessões ativas e tentativas de login;
- Mantenha apenas instalados os softwares que são utilizados. Não instale softwares inúteis, como desfragmentadores para sistemas Linux, pois o Linux não necessita ser desfragmentado;
- Sempre remova os metadados antes de compartilhar algo;

- Em celulares, VPNs são menos eficazes que em notebooks;
- Não compartilhe informações pessoais na dark net ou que possibilitem o cruzamento de diferentes identidades;
- Não se gabe por seus feitos em fóruns, mesmo que tenham sido algo realmente bacana;
- Evite configurar navegadores comuns para utilizar o proxy da rede Tor. Use o Tor Browser;
- Nunca entre pela internet normal em contas que você entrou usando uma rede do tipo onion;
- De maneira geral, um proxy é inferior a uma VPN, que é inferior a uma rede do tipo onion;
- Pelas características de arquitetura dos sistemas operacionais modernos, smartphones são mais seguros que computadores tradicionais, mesmo sendo menos privados. Atualizar softwares não apenas mitiga vulnerabilidades conhecidas e corrigidas, novas versões, por exemplo, do Android, trazem melhorias contínuas à segurança do sistema. Versões mais novas do Android são mais seguras que versões mais antigas;
- Por meio do número de telefone é possível derivar uma identidade, pois, a cada conexão realizada às antenas dos serviços de telefonia, os identificadores do dispositivo e do cartão SIM são enviados, possibilitando conhecer a localização do usuário. Evite ligar uma identidade aos identificadores, comprando o dispositivo e o cartão SIM de forma anônima, se possível;
- Remover o SIM dificulta o rastreamento. No entanto, trocar o SIM, mas continuar utilizando o mesmo dispositivo não impede a correlação de identidades, devido aos identificadores do próprio dispositivo;
- Instale uma ROM customizada em seu dispositivo móvel. Mesmo com opções como Lineage e Calyx, o recomendado é o GrapheneOS, instalado em dispositivos Pixel, da Google. Os Pixel possuem bom grau de segurança em hardware, mas pouca privacidade. Com a instalação do GrapheneOS, o dispositivo torna-se um dos celulares mais seguros, privados e anônimos já concebidos, muito superior aos antigos BlackBerries;
- Para alguns contextos, talvez não seja vantajoso o uso de telefones celulares;
- Caso precise utilizar sua voz em uma live ou vídeo, por exemplo, tente modificá-la com o uso de softwares como o Lyrebird;
- Para contas anônimas, pode-se utilizar imagens do site https://thispersondoesnotexist.com/;
- Evite postar fotos verdadeiras que mostrem seu rosto. Em posse de apenas uma imagem sua, é trivial encontrar todas as vezes que seu rosto apareceu na internet;

- Sempre vá na documentação oficial do serviço para obter as corretas e atualizadas instruções de instalação;
- Não instale softwares de sites não oficiais ou com reputação duvidosa. Quando possível, verifique a autenticidade do software baixado por meio das chaves criptográficas. Para cada situação, as instruções podem ser encontradas na documentação oficial dos serviços;

## Dicas e Pontos Gerais Para o Mundo Físico

- Planeje antes de executar. Alterações sempre precisarão ser realizadas, mas sempre tenha um escopo mais ou menos definido. Planejamento é fundamental para evitar que erros do passado, que agora não podem mais ser corrigidos, voltem para te morder;
- Nunca deixe um laptop sozinho, mas, se o fizer, em vez de apenas abaixar a tampa, desligue-o. Isso dificulta o vazamento de informações para adversários com acesso ao seu dispositivo, por exemplo, as informações presentes na memória RAM. Espere alguns minutos após o desligamento para poder se afastar do computador, esse tempo é suficiente para que dados presentes na memória volátil sejam apagados;
- Desconecte dispositivos criptografados após o uso;
- Para a completa mitigação dos dados presentes em um dispositivo de armazenamento, a destruição física é a opção ideal. Contudo, deve ser feita da maneira correta. Caso pedaços grandes, por exemplo, do HDD permaneçam intactos, dados podem ser obtidos mesmos desses pedaços. Cartões SIM podem ser colocados no micro-ondas. Os dispositivos podem ser queimados, porém, certifique-se de que o dispositivo propriamente dito, não apenas a capa ou encase, foram queimados e destruídos;
- Forças policiais podem te obrigar a usar biometria para acessar seus dispositivos. Utilizar uma senha impede que sejam desbloqueados forçadamente com o seu dedo ou rosto;
- Em ambientes hostis, evite circular a pé sem proteção de identidade ou com meios de transporte que facilmente podem levar a você, como o seu carro;
- Use rotas diferentes para chegar ao mesmo local;
- Em protestos, não leve seu smartphone, ou deixe-o em uma Faraday Bag. Por meio dos celulares, forças policiais podem derivar a identidade de todos os que presencialmente participaram;
- Pode-se utilizar celulares descartáveis, para situações específicas;
- Caso seja necessário, remova fisicamente câmeras e microfones de seus dispositivos móveis;
- Para dificultar o rastreamento e identificação facial, cubra o rosto com uma máscara, bandana e/ou óculos escuros. Analise cada situação e verifique se, naquele contexto, você chamará mais atenção do que gostaria;
- Câmeras com inteligência artificial podem analisar o modo de andar. Mesmo com o rosto coberto e diferentes disfarces, esse parâmetro pode ser utilizado contra você. Utilize uma combinação sempre diferente de meias e palmilhas, pois elas modificarão o seu andar e dificultarão a correlação por essa métrica;

- O uso de sua voz em redes monitoradas, como a telefônica, instantaneamente te identifica. Evite realizar ligações não criptografadas e comunicação por SMS;
- Cubra tatuagens, retire anéis, piercings e joias; tudo aquilo que possa facilmente te identificar;
- Quando em trânsito, coloque todos os dispositivos em Faraday Bags;
- Embalar dispositivos em alumínio bloqueia a transmissão de certas frequências, mas é uma solução inferior a uma Faraday Bag, pois o dispositivo pode não ficar tão bem embrulhado, não bloquear com sucesso a mesma faixa de frequências abrangidas por um tecido de maior qualidade, além de ser uma solução menos discreta;
- Utilize roupas não chamativas;
- Não chame atenção, ganhe anonimato pela multidão. Seja publicamente desinteressante;
- A região entre os olhos e superior do nariz é importante para o reconhecimento facial, cubra-a;
- Tenha sempre uma muda de roupas reserva para trocar quando preciso. Troque o estilo e enseie modificação rápida de visual;
- Não utilize aplicativos de transporte, como Uber;
- Utilize meios não rastreáveis de transação, como metais (prata), criptomoedas (Monero) e dinheiro em espécie. Certifique-se da presença de câmeras antes de realizar transações;
- Analise a presença de câmeras nos trajetos percorridos e tente descobrir pontos cegos;
- Quando utilizar seus dispositivos em espaços públicos, certifique-se de se posicionar de uma maneira que dificulte a extração de informações. Prefira ficar de costas para uma parede em vez de para uma janela, por exemplo;
- Coloque os parafusos do notebook em uma posição conhecida ou coloque uma camada de tinta que será danificada caso houver uma tentativa de abertura;
- Não possua dispositivos IOT, como os assistentes domésticos, ou outros dispositivos vestíveis, como smart watches;
- Tenha meios não tecnológicos de identificar que alguém esteve em sua casa ou local de temporário de abrigo. Em caso de suspeita, verifique a presença de câmeras e microfones instalados. Planeje os próximos passos nesse tipo de situação;

- Fabricantes de notebooks voltados à privacidade, como a Purism, utilizam softwares e drivers de código aberto e realizam modificações ao nível de hardware. Nos dispositivos da Purism, por exemplo, interruptores que fisicamente desconectam chips internos são utilizados para garantir que nenhuma comunicação está sendo realizada. Em seus notebooks, existem interruptores para webcam e microfone, bem como Wi-Fi e Bluetooth. Além da Purism, fabricantes como a System 76 neutralizam a possível *backdoor* instalada em todos os processadores Intel, o chamado Intel Management Engine (ME);
- Evite imprimir documentos sigilosos em impressoras que podem ser ligadas a você, pois impressoras podem imprimir minúsculos pontos nas folhas impressas que são capazes de identificar em que equipamento ocorreu a impressão. Não se sabe qual a porcentagem de impressoras que realizam essa prática. Uma maneira barata de identificar os pontos é com o uso de uma luz azul;
- Espelhos podem esconder câmeras ocultas. Não utilize espelhos inteligentes;
- Não discuta assuntos sensíveis próximo a dispositivos inteligentes, como os equipados com Alexa;
- Utilize criptografia de qualidade onde, quando e sempre quando for possível. Sempre que possível, compartimentalize suas atividades.

## Softwares/serviços recomendados

- Aegis
- BleachBit (HDD)
- Briar
- Cryptocam
- CryptPad
- DroidFS
- DuckDuckGo (https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/)
- ExifCleaner
- Metadata Cleaner (para limitar o risco de corrupção dos arquivos, escolha a opção de limpeza leve)
- F-droid
- Haven
- InviZible Pro
- KeePassXC
- NetGuard
- Nextcloud
- ObscuraCam
- Phobos (https://phobosxilamwcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id.onion/)
- Photok
- RethinkDNS
- Safe Notes
- SecureDrop (sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion)
- Session
- Speek!
- Standard Note
- VeraCrypt

**Gabriel Camargo**

## POPULARES

**58 Privilégios das mulheres na sociedade ocidental**

18/01/2019

**O site de e-books piratas Z-Library desaparece – deixando estudantes universitários em pânico**

05/11/2022

**Guia de Criptomoedas para Iniciantes V2.0**

06/04/2019

## POPULARES

**Entretenimento Financeiro – A Festa do Dinheiro Para Todos**

01/03/2023

**O Bitcoin é “tipo whatsapp, só que diferente”**

28/02/2023

**O que um Reality Show pode nos mostrar sobre Sistemas Legais?**

05/03/2023

## LEIA TAMBÉM

**O Bitcoin é “tipo whatsapp, só que diferente”**

28/02/2023

**Quando o mel é bom “o estado sempre toma”**

03/03/2023

**Lula decide taxar videogames para compensar corte no IR**

02/03/2023

## CATEGORIAS

| | |
|---|---|
| Política | 402 |
| Economia | 255 |
| Criptomoedas | 255 |
| Ética | 159 |
| Direito | 81 |
| Cultura | 27 |
| Tecnologia | 14 |

gazetalibertária.

## SOBRE NÓS

Nosso objetivo é levar notícias, opinião, análises e informações sobre política, economia, ética e direito com honestidade e transparência, sob uma perspectiva austrolibertária e comprometimento com a verdade.

APOIE A GAZETA LIBERTÁRIA

Contato: gazeta@universidadelibertaria.com

## SIGA-NOS

Domínio Público, não acreditamos em propriedade intelectual.